WHAT IS CLAIMED IS:

1.   A test mechanism for testing device driver hardening, the test mechanism comprising an intercept mechanism for intercepting device access calls from a
5 device driver under test and an interface for configuring the intercept mechanism for faults to be injected in response to the device access calls according to a determined test pattern.

2.   The test mechanism of claim 1, wherein the intercept mechanism comprises
10 a plurality of intercept routines.

3.   The test mechanism of claim 2, wherein each intercept routine is for a given type of device access call.

15 4.   The test mechanism of claim 2, comprising a mapping mechanism for mapping device access calls to intercept routines.

5.   The test mechanism of claim 4, wherein the mapping mechanism comprises a look-up table.
20

6.   The test mechanism of claim 1, wherein the intercept mechanism is operable to monitor device access calls to determine when to inject a fault.

7.   The test mechanism of claim 1, comprising a counter associated with at least
25 one predetermined type of device access call, the intercept mechanism being configured to monitor the counter which is modified for each device access call of that type, and to be operable to inject a fault in response to a determined count of the counter.

8.   The test mechanism of claim 7, comprising a second counter for determining a number of times a fault is to be injected for successive device access calls of the predetermined type.

5   9.   The test mechanism of claim 3, wherein each type of device access call is separately monitored.

10.   The test mechanism of claim 1, wherein a device access infrastructure is responsive to a device access call to intercept the call for the selective insertion of
10   faults and the intercept mechanism is operative to return an emulated device response.

11.   The test mechanism of claim 1, wherein a device access infrastructure is responsive to a device access call to intercept the call and the intercept mechanism
15   is operable to provide selective insertion of faults prior to effecting the device access.

12.   The test mechanism of claim 11, wherein the intercept mechanism operates on data of a device access call with a determined operator and operand.
20

13.   The test mechanism of claim 6, wherein the interface is operable to configure the intercept mechanism for determining when the intercept mechanism injects a fault.

25   14.   The test mechanism of claim 1, wherein the interface comprises an application program interface responsive to a test application for determining a test pattern.

15.   A test application on a carrier medium for a test mechanism according to
30   claim 14, the test application comprising computer code configured to be operable:

to provide the interface with a test configuration;

to detect the response of a device driver to a test condition inserted by the intercept mechanism;

to compare the detected response to an expected response set out in a test
5 script; and

to identify discrepancies between the detected response and the expected response.

16.   The test application of claim 15, wherein the test application comprises
10 computer code configured to be operable to maintain a log of the detected responses.

17.   (A computer program product on a carrier medium, the computer program product comprising an intercept mechanism for intercepting device access calls from
15 a device driver under test and an interface for configuring the intercept mechanism for faults to be injected in response to the device access calls according to a determined desired test pattern.

18.   A test mechanism for testing device driver hardening, the test mechanism
20 comprising a means for intercepting device driver access calls from a device driver under test and means for injecting a fault in a response to the device access call according to a determined test pattern.

19.   A computer comprising a device driver for accessing an I/O device and a
25 test mechanism for testing device driver hardening, the test mechanism comprising an intercept mechanism for intercepting device access calls from a device driver under test and an interface for configuring the intercept mechanism for faults to be injected in response to the device access calls according to a determined test pattern.

20.　　A method of testing the hardening of a device driver, the method comprising intercepting device driver access calls from the device driver and injecting a fault in a device driver access according to a desired test pattern.

5　21.　　The method of claim 20, comprising a mapping the device access call to at least one intercept routine for handling the device access call.

22.　　The method of claim 21, comprising mapping a device access call to an intercept routine according to a device access call type.

10

23.　　The method of claim 20, comprising monitoring device access call to determine when to inject a fault.

24.　　The method of claim 23, comprising modifying a count for each device

15　access call of a given type and injecting a fault in response to predetermined count being attained.

25.　　The method of claim 24, comprising separately monitoring each type of call.

20　26.　　The method of claim 24, comprising a further step of monitoring a number of times the fault is to be injected in sequence.